UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00101

CISCO PRIVILEGE ESCALATION BUGS

DATE ISSUED: 2nd February 2021

IMPACT	LOW	[✓ MEDIUM]	HIGH
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

Cisco is currently investigating a vulnerability discovered to affect several of their products using the Sudo command line code.

BREAKDOWN

Due to improper parsing of the command line parameters, using the Sudo command an attacker may be able to access a Unix shell of any affected device. "Sudoedit" used in conjunction with specially designed parameters or a binary exploit, an attacker can take advantage of this vulnerability and create a heap-based buffer overflow attack. Cisco is not aware of any active exploitation of the vulnerability at this stage, and a number or products remain under investigation. Cisco have noted the following products to be vulnerable to the exploit and have included bug IDs which are searchable through the Cisco Bug Search Tool:

Cisco FXOS Software – CSCvx21208

Cisco Prime Collaboration Provisioning – CSCvx18714

Cisco Nexus 3000 series switches and 9000 series switches in standalone NX-OS mode – CSCvx18710

REMEDIATION STEPS

- Ensure devices that require an update have sufficient memory and check that existing configuration will remain supported after upgrade before applying security patches.
- Apply available software upgrades supplied by Cisco.
- Consult with a Cisco representative or reseller if you have any further questions or concerns.

REFERENCES & RESOURCES

Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sudo-privesc-jan2021-qnYQfcM
Mitre	https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3156